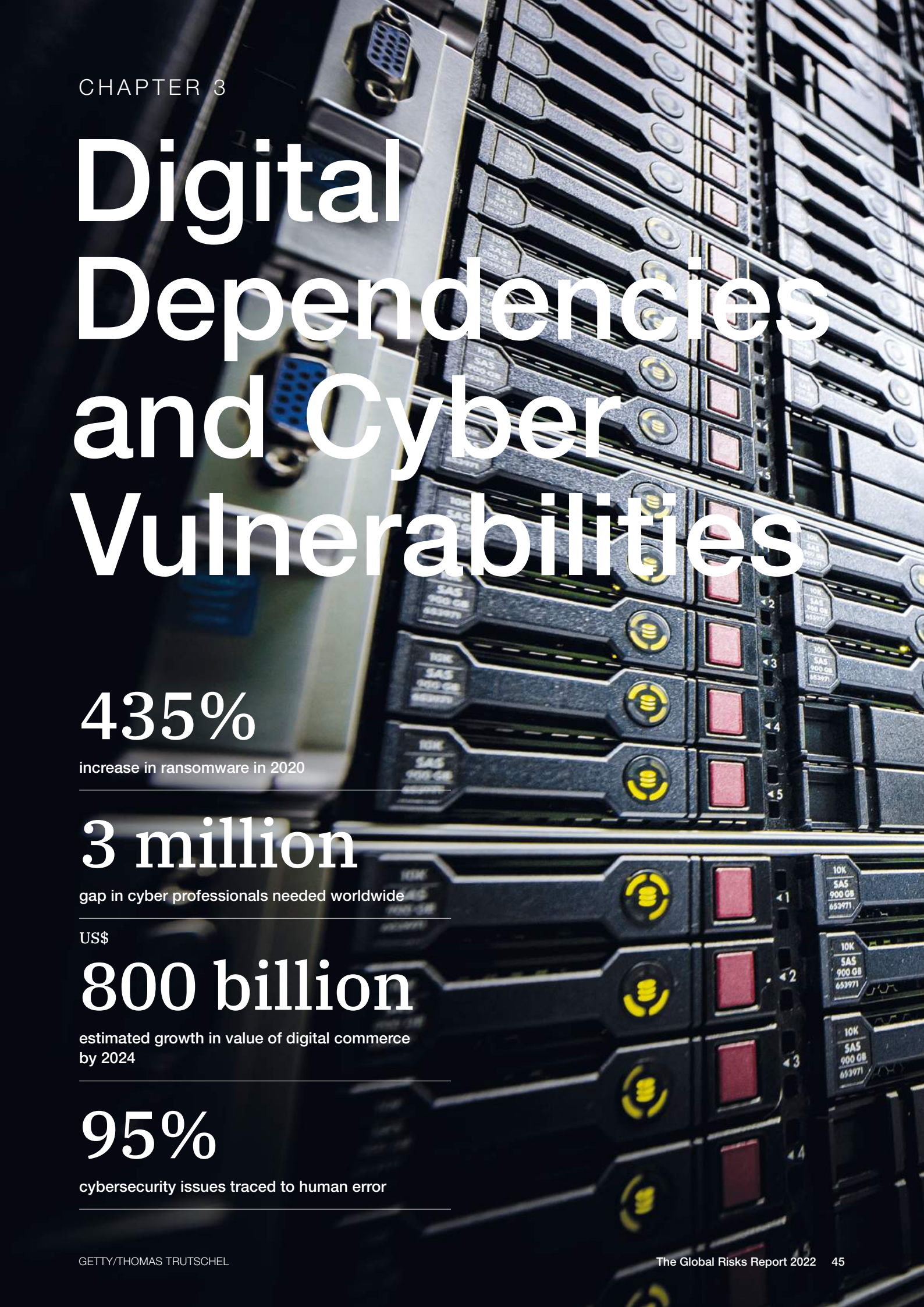
CHAPTER 3

Digital Dependencies and Cyber Vulnerabilities



435%

increase in ransomware in 2020

3 million

gap in cyber professionals needed worldwide

US$ 800 billion

estimated growth in value of digital commerce by 2024

95%

cybersecurity issues traced to human error

GETTY/THOMAS TRUTSCHEL

Digital distress

Governments, societies and companies increasingly rely on technology to manage everything from public services to business processes, even routine grocery shopping.[1] Converging technological platforms, tools and interfaces connected via an internet that is rapidly shifting to a more decentralized version 3.0 are at once creating a more complex cyberthreat landscape and a growing number of critical failure points. As society continues to migrate into the digital world, the threat of cybercrime looms large, routinely costing organizations tens—even hundreds—of millions of dollars. The costs are not just financial: critical infrastructure, societal cohesion and mental well-being are also in jeopardy.

Digital everything

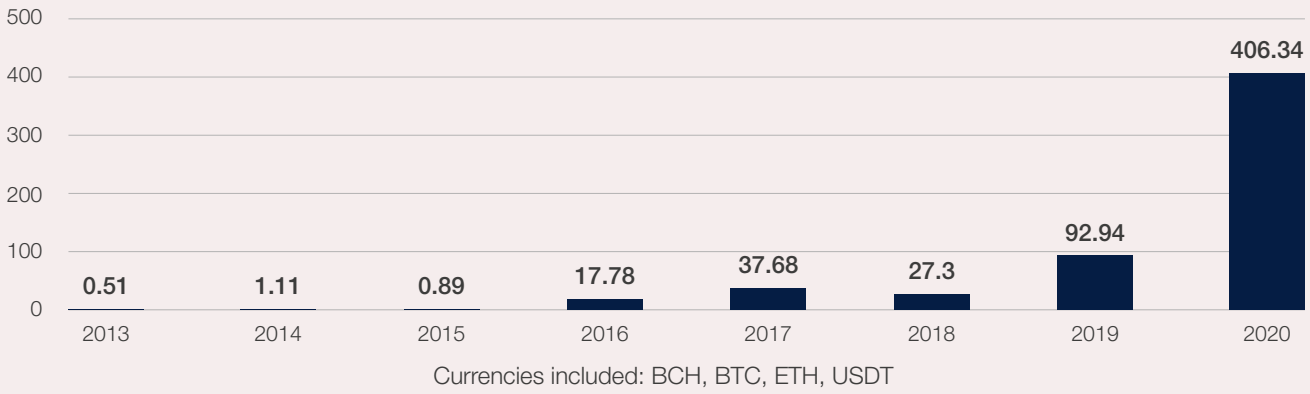
Growing dependency on digital systems over the last 20 years has drastically shifted how many societies function.[2] The COVID-19-induced shift to remote work has accelerated the adoption of platforms and devices that allow sensitive data to be shared with third parties—cloud service providers, data aggregators, application programming interfaces (APIs) and other technology-related intermediaries.[3] These systems, while powerful tools for data and processing, attach an additional layer of dependency on service providers. Remote work has also moved digital exchanges from office networks to residential ones, which have a greater variety of connected devices with less protection against cyber intrusion. In parallel, the appetite for capabilities predicated upon using multiple technologies working in concert—including artificial intelligence (AI), Internet of Things (IoT)/ Internet of Robotic Things–enabled devices, edge computing, blockchain and 5G—is only growing.[4] While these capabilities afford tremendous opportunities for businesses and societies to use technology in ways that can dramatically improve efficiency, quality and productivity, these same capabilities also expose users to elevated and more pernicious forms of digital and cyber risk.

In the future, the interconnectedness and convergence of these digital tools will continue to increase as society embraces the next version of the internet built upon blockchain technology. One manifestation of this migration will be the metaverse: a network of 3D virtual spaces, enabled by cryptocurrencies and non-fungible tokens (NFTs) among other technologies, with unprecedented socio-economic interoperability and immersive virtual reality experiences.[5] Users will be required to navigate security vulnerabilities inherent in both increased dependency on and growing fragmentation in these types of complex technologies often characterized by decentralization and lack of structured guardrails or sophisticated onboarding infrastructure.

GETTY/FILIPPOBACCI

FIGURE 3.1

Total Cryptocurrency Value Received by Ransomware Addresses, 2013-2020



Source: Based on Chainanalysis. Ransomware 2021: Critical Mid-Year Update. Insights blog. https://blog.chainalysis.com/reports/ransomware-update-may-2021

Cyber vulnerabilities

In the context of widespread dependency on increasingly complex digital systems, growing cyberthreats are outpacing societies' ability to effectively prevent and manage them. For example, the digitalization of physical supply chains creates new vulnerabilities because those supply chains rely on technology providers and other third parties, which are also exposed to similar, potentially contagious, threats.[6] In December 2021, just one week after discovering a critical security flaw in a widely used software library (Log4j), more than 100 attempts at exploiting the vulnerability were detected every minute, illustrating how free access coding can spread vulnerabilities widely.[7] Information technology (IT) monitoring and management software also illustrate the potential for contagious exposure, which can break through the defences of critical cybersecurity supply chains, as shown by the Solar Winds Orion attack that occurred in late 2020.[8] While a state-based institution with highly sophisticated capabilities probably lodged this attack, other criminal organizations will certainly attempt to replicate this approach.[9] At the same time, older vulnerabilities persist with many organizations still relying on outdated systems or technologies.

Malicious activity is proliferating, in part because of the growing vulnerabilities—but also because there are few barriers to entry for participants in the ransomware industry and little risk of extradition, prosecution or sanction.[10] Malware increased by 358% in 2020, while ransomware increased by 435%,[11] with a four-fold rise in the total cryptocurrency value received by ransomware addresses (see Figure 3.1).[12] "Ransomware as a service" allows even non-technical criminals to execute attacks, a trend that might intensify with the advent of artificial intelligence (AI)-powered malware.[13] In fact, profit-seeking groups of cyber mercenaries stand ready to provide access to sophisticated cyber-intrusion tools to facilitate such attacks. Furthermore, cryptocurrencies have also allowed cybercriminals to collect payments with an only modest risk of detection or monetary clawback.[14]

Attacks themselves are also becoming more aggressive and widespread.[15] Cyberthreat actors using ransomware are leveraging tougher pressure tactics as well as going after more vulnerable targets, impacting public utilities, healthcare systems and data-rich companies.[16] For example, before it disbanded, DarkSide—the group accused of being responsible for the Colonial Pipeline attack—offered a suite of services ("triple" or "quadruple" extortion)

REUTERS/JIM YOUNG

to clients beyond simply encrypting files; these included data leaks and distributed denial-of-service (DDoS) attacks. Hacker groups will also contact victims' clients or partners to get them to urge the victims to pay ransoms. Among the services offered is the collection of top executive information for blackmail.[17]

Sophisticated cyber tools are also allowing cyberthreat actors to attack targets of choice more efficiently, rather than settling for targets of opportunity, highlighting the potential to carry out more goal-oriented attacks that could lead to even higher financial, societal and reputational damage in the future. Increasingly sophisticated use of spyware technologies, for example, has allowed for targeted attacks against journalists and civil rights activists across geographies—spurring a wave of political and industrial blowback in the form of government sanctions and lawsuits.[18] The ability to tailor attacks at will includes timing them for when cybersecurity teams and leadership could be distracted by other priorities, such as during peak COVID-19 outbreaks or a natural disaster. Cyberthreat actors are also accessing higher-quality and more sensitive information from victims. And deepfake technology is allowing cyberthreat actors to improve social engineering ploys, proliferate disinformation and wreak societal havoc, especially at times of high volatility.[19]

Global Risks Perception Survey (GRPS) respondents reflect these trends, ranking "cybersecurity failure" among the top-10 risks that have worsened most since the start of the COVID-19 crisis. Moreover, 85% of the Cybersecurity Leadership Community of the World Economic Forum have stressed that ransomware is becoming a dangerously growing threat and presents a major concern for public safety.[20] At a regional level, "cybersecurity failure" ranks as a top-five risk in East Asia and the Pacific as well as in Europe, while four countries—Australia, Great Britain, Ireland and New Zealand—ranked it as the number one risk. Many small, highly digitalized economies—such as Denmark, Israel, Japan, Taiwan (China), Singapore and the United Arab Emirates—also ranked the risk as a top-five concern.

Already-stretched IT and cybersecurity professionals are under an increasing burden, not only because of the expansion of remote work but also because of the growing complexity of regulations for data and privacy, even though such regulations are critical to ensuring public trust in digital systems.[21] There is an undersupply of

"Cybersecurity failure" is one of the risks that worsened the most through COVID-19

cyber professionals—a gap of more than 3 million worldwide[22]—who can provide cyber leadership, test and secure systems, and train people in digital hygiene.[23] As with other key commodities, a continued lack of cybersecurity professionals could ultimately hamper economic growth,[24] although new initiatives to "democratize" cybersecurity, for example, by providing free cybersecurity risk management tools, could help fill some of the gaps for small businesses or other institutions.[25]

There are concerns that quantum computing could be powerful enough to break encryption keys—which poses a significant security risk because of the sensitivity and criticality of the financial, personal and other data protected by these keys. The emergence of the metaverse could also expand the attack surface for malicious actors by creating more entry points for malware and data breaches.[26] As the value of digital commerce in the metaverse grows in scope and scale—by some estimates projected to be over US$800 billion by 2024—these types of attacks will grow in frequency and aggression.[27] The myriad forms of digital property such as NFT art collections and digital real estate could further entice criminal activity.

For governments attempting to prevent cybersecurity failures, patchwork enforcement mechanisms across jurisdictions continue to hamper efforts to control cybercrime.[28] Geopolitical rifts hinder potential cross-border collaboration, with some governments unwilling or unable to regulate cyber intrusions that originate inside and impact outside their borders. Unsurprisingly, given the geopolitical tensions around digital sovereignty, according to GRPS respondents, "cross-border cyberattacks and misinformation" and "artificial intelligence" were among the areas with the least "established" or "effective" international risk mitigation efforts.

Companies must also act ahead of new regulatory shifts, as the political undercurrents/geopolitical tensions between various countries might impact cross-border data flows. This might mean moving data processing to jurisdictions that might allow for better customer protection around data privacy issues.[29]

Consequences

Often-repeated examples of past cyber intrusions are worth re-examination, as these cases demonstrate how damaging attacks on large and strategically significant systems—such as banking, hospital, Global Positioning System (GPS) or air traffic control systems—could be.[30] As resources are increasingly digitized, notable as well is the heightened risk of cyber espionage attacks that typically target intellectual property and result in high developmental and reputational costs to both private and public sector organizations.[31]

The interaction between digitalization and growing cyberthreats carries intangible consequences as well. The growth of deepfakes and "disinformation-for-hire" is likely to deepen mistrust between societies, business and government.[32] For example, deepfakes could be used to sway elections or political outcomes.[33] More concretely, in one recent case, cybercriminals cloned the voice of a company director to authorize the transfer of US$35 million to fraudulent accounts.[34] There is also a booming market for services designed to manipulate public opinion in favour of clients, public or private, or to damage rivals.[35] Fraud, too, will become easier and therefore more frequent with banking, health and civic processes going remote.

Patchwork enforcement mechanisms continue to hamper efforts to control cybercrime

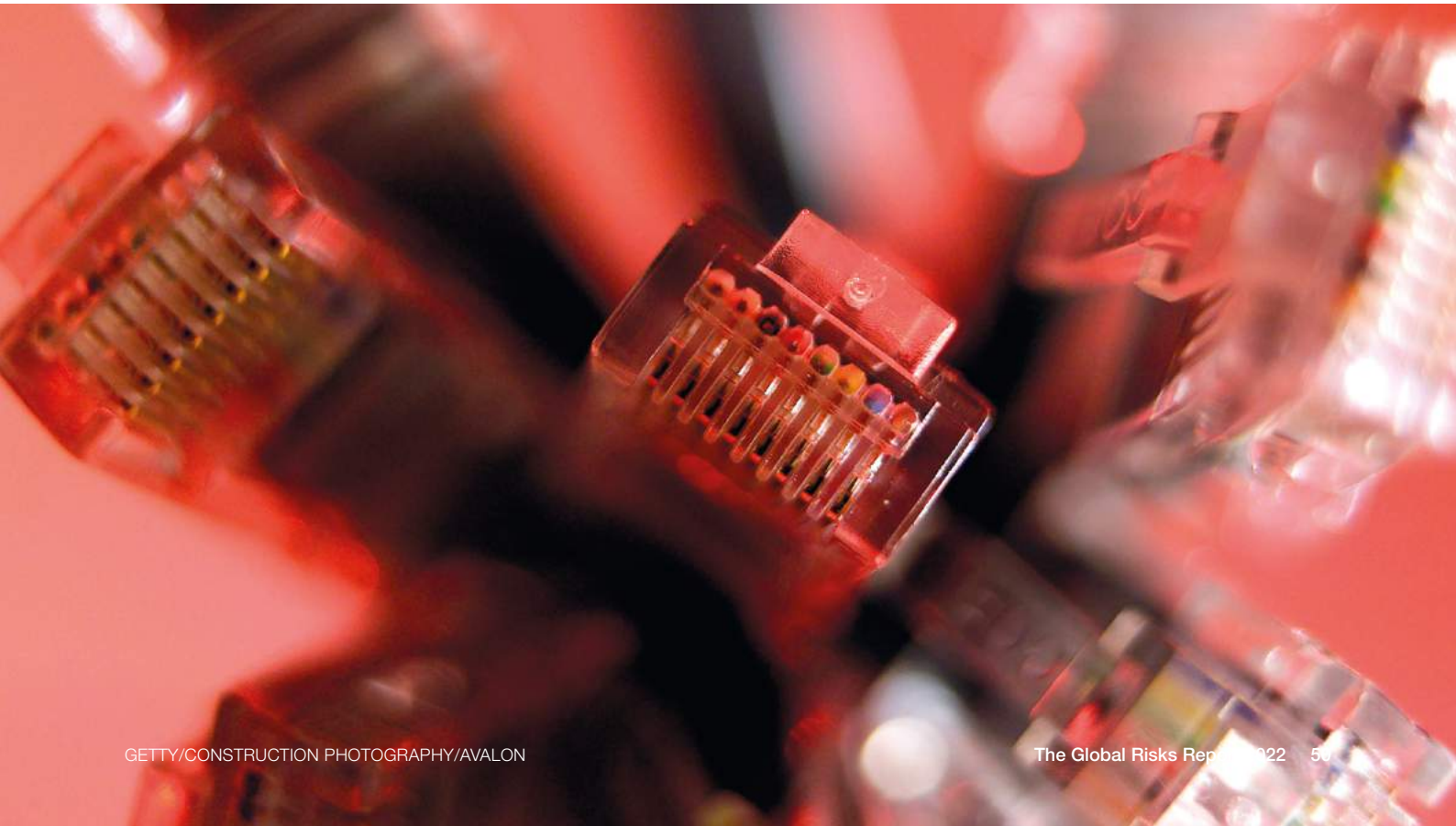
In 2021, UK internet banking fraud rose by 117% in volume and 43% in value compared with 2020 levels, as people spent more time shopping online.[36] Digital safety overall—from health misinformation and extremism to child exploitation—faces new challenges with unexperienced and more vulnerable populations coming online.[37]

Even in the best-case scenario of aggressive digital threat defences, there will be significant increases in the cost of operations for all stakeholders. This could be particularly challenging for small- or medium-sized businesses that might spend 4% or more of their operational budget on security, compared to larger organizations that might spend closer to 1–2%.[38] Indeed, amid the rising frequency and severity of ransomware claims, cyber insurance pricing in the United States rose by 96% in the third quarter of 2021, marking the most significant increase since 2015 and a 204% year-over-year increase.[39] Respondents to the GRPS indicate a long-term concern with these developments, with "adverse tech advances" appearing as a top-10 risk over a 5-to-10-year horizon.

Cyberthreats also continue to drive states apart, with governments following increasingly unilateral paths to control risks. As attacks become more severe and broadly impactful, already-sharp tensions between governments impacted by cybercrime and governments complicit in their commission will rise as cybersecurity becomes another wedge for divergence, rather than cooperation, among nation states.[40] Particularly in an era of rising tensions between superpowers, cyberattacks are another battlefront in which escalation is a key risk (see Chapter 1).[41] If cyberthreats continue without mitigation, governments will continue to retaliate against perpetrators (actual or perceived), leading to open cyberwarfare, further disruption for societies and loss of trust in governments' ability to act as digital stewards.

Digital security divides: Consequences for people

Among the most vulnerable are those who are only now coming online or will soon do so. Around 40% of the world's population is not yet connected to the internet.[42] These individuals are already facing inequalities in digital security, which will only widen with the advent of internet 3.0 and the metaverse.[43] Within digitally advanced societies, vulnerable populations are also often more digitally at risk: for example, a recent study finds that low-income residents of San Francisco—

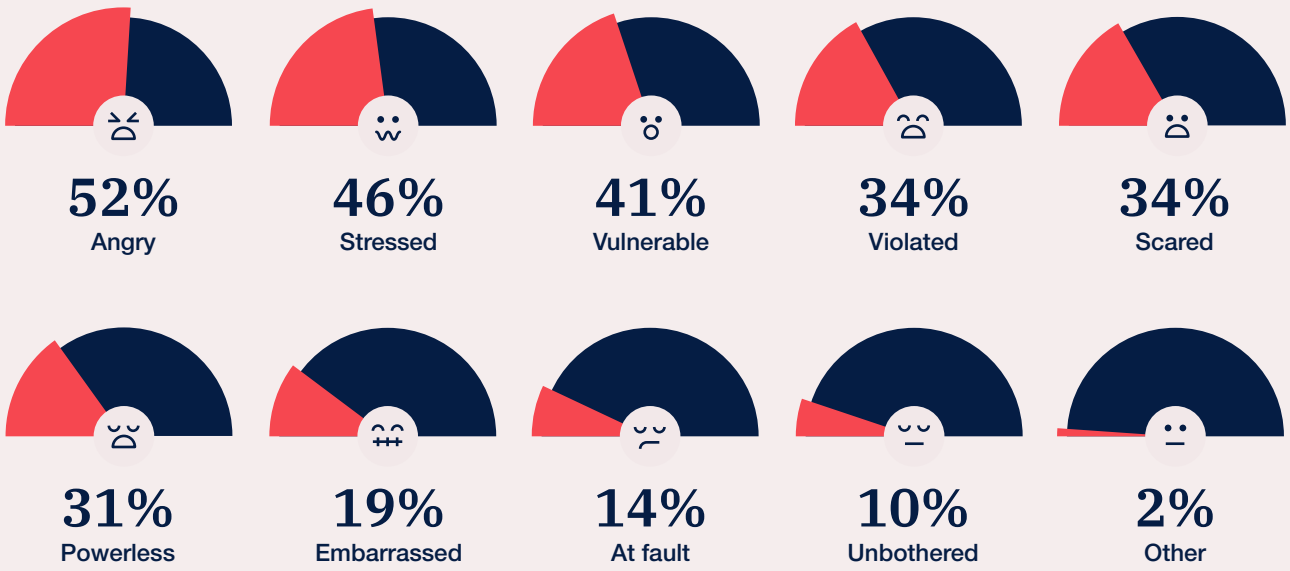


GETTY/CONSTRUCTION PHOTOGRAPHY/AVALON

FIGURE 3.2

Emotions Experienced after Detecting Unauthorized Access

Global total of those who detected unauthorized access in past 12 months



Source: NortonLifeLock Inc. 2021. "2021 Norton Cyber Safety Insights Report: Global Results". Norton and The Harris Poll. May 2021. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

the cultural heart of Silicon Valley—are more likely than wealthier residents to be cybercrime victims.[44] In other situations, obligatory digital identity markers could introduce new risks for citizens, particularly evident in the growing risk that deepfakes could compromise biometric authentication.[45]

Individuals will increasingly experience anxiety as control over their data becomes more precarious and they are subjected to personal attacks, fraud, cyberbullying and stalking (see Figure 3.2).[46] A perceived lack of agency could also lead to apathy in taking responsibility for securing one's own digital footprint, as evinced by the continued market dominance of instant messenger applications plagued by privacy controversies.[47] Even with more widespread "reject all" options on websites intended to simplify personal data privacy, there are drawbacks and caveats—such as limiting functionality and other options. Importantly, these features are just a tiny part of the larger privacy equation. Websites are still littered with tracking pixels and third-party scripts that remain powerful ways to fingerprint online behaviours.[48]

Overreaching or underdelivering: Consequences for governments

Government at all levels faces mounting responsibilities and many are struggling to uphold their end of the digital social contract: securing critical infrastructure; addressing threats to "epistemic security" from disinformation; protecting the integrity of civic processes and public services; legislating against cybercrime; training and educating populaces around cyber literacy; regulating digital service providers; and ensuring the availability of resources, such as rare-earth minerals, for the digital economy. The necessary oversight could lead to overreach as governments move to shut down systems, erect higher digital barriers or embark on digital colonization (by monopolizing digital systems) for geopolitical ends.[49] While such actions might carry the ostensible goal of reducing

attacks and disruption, these policies could quickly become a vehicle for oppression. Already suffering from a loss in public trust as a result of the COVID-19 crisis, governments may face further societal anger if they are unable to both keep up with the shifting threat landscape and responsibly manage these challenges.

Pay, protect or perish: Consequences for businesses

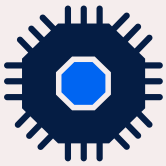
As cyberthreats continue to grow, insuring against such risks will become increasingly precarious, with insurers themselves facing retaliatory attacks for attempting to curb ransomware payments.[50] Thus, when an attack occurs, businesses will either be forced to pay increasingly high ransoms or suffer the reputational, financial, regulatory and legal consequences of cyberattacks. As previous incursions (like SolarWinds) have demonstrated, exposure to vendors and supply chain partners must also be assessed and managed. The impact of disruptive cyberattacks could be financially devastating for businesses that fail to invest in protections for their digital infrastructure, particularly in a scenario in which governments begin prohibiting ransom payments or penalizing poor cybersecurity practices.[51] Furthermore, as environmental, social and governance (ESG) concerns come increasingly into focus (see Chapter 2), businesses that fail to demonstrate strong corporate governance around cybersecurity—such as by implementing robust systems and process oversight protocols, and by practicing accountability and transparency in the event of a breach—could suffer reputational harm in the eyes of ESG-focused investors.

Businesses also operate in a world in which 95% of cybersecurity issues can be traced to human error,[52] and where insider threats (intentional or accidental) represent 43% of all breaches.[53] Some companies will inevitably move to greater segmentation of digital systems to better account for insider risk. Companies could begin or continue to lock up key data as a result of the cybersecurity issues. Workforce efficiency, too, could suffer if accessing data and information is less seamless.

Shocks to reflect upon

NotPetya 2.0

What if an attack that is even more wide-ranging and costly than NotPetya—with the ability to self-propagate and even mutate to avoid preventative controls—created cascading lockups of systemically important businesses, bankrupting organizations, disrupting services and unwinding the digital transformation efforts made over the past years?



Sovereignty slips

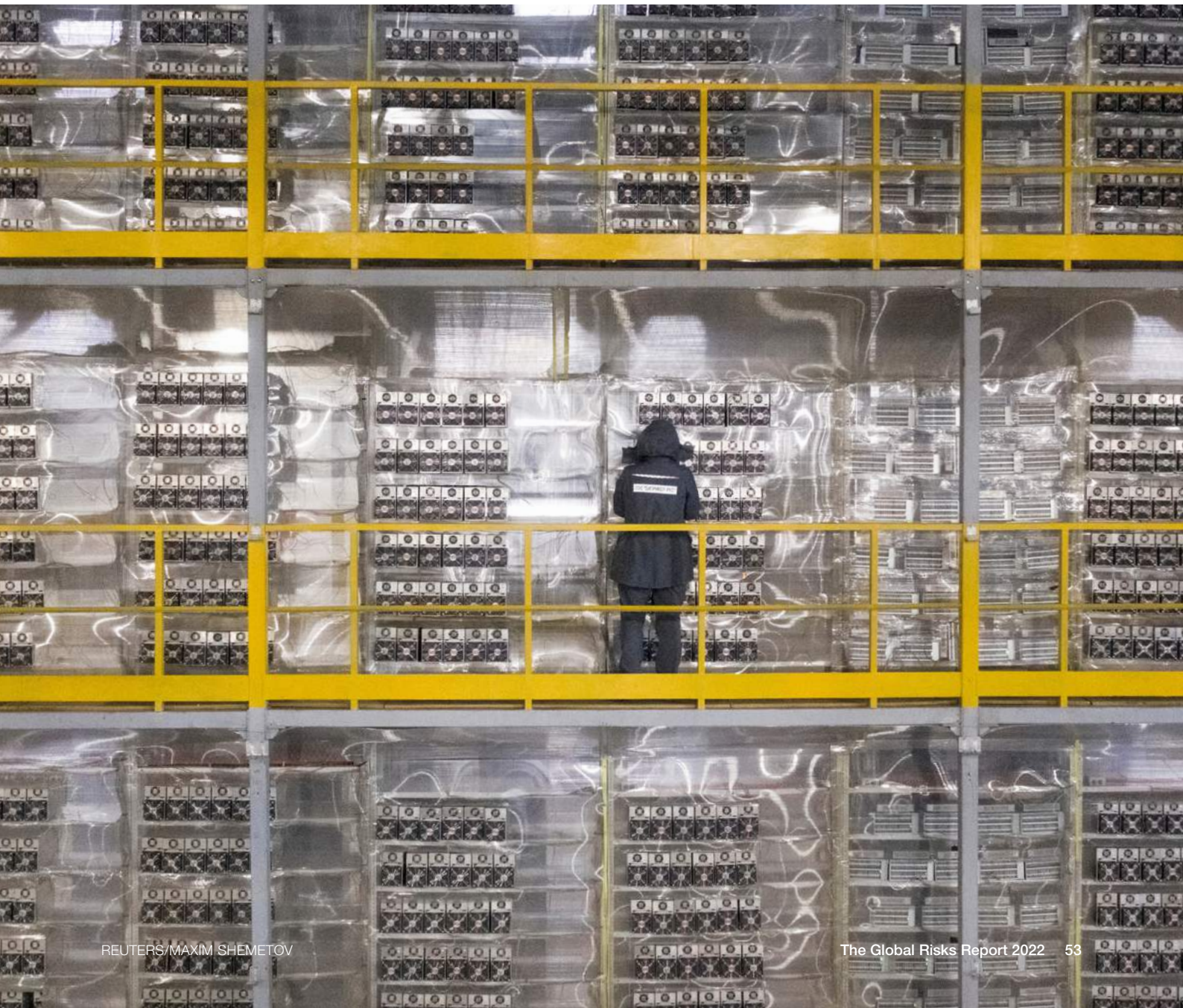
What if the shifts towards privately held IT infrastructure as well as cryptocurrency and decentralized finance undermine governments' control over data, processes and financial systems?

Undetected disruption

What if subtle changes in health, banking or other data go undetected for years, but carry significant consequences for premature death, loss of funds or other significant consequences over time? How can cyber espionage compromise return on R&D investment and competitiveness in the future?

Towards greater cyber resilience

As our reliance on digital technologies grows and Internet 3.0 becomes reality, efforts aimed at building norms and defining rules of behaviour for all stakeholders in cyberspace are intensifying. While multistakeholder international dialogues can help strengthen links between actors operating in the digital security realm, cooperation between organizations could unlock best practices that can be replicated across industries and economies. Initiatives should focus on emerging technologies, such as blockchain, quantum and artificial intelligence, as well as the modes of digital exchange they facilitate, like the metaverse. Leaders must remain attentive to perennial concerns like cybercrime and ransomware attacks as well. At the organizational level, upskilling leaders on cybersecurity issues and elevating emerging cyber risks to board-level conversations will strengthen cyber-resilience. In a deeply connected society, digital trust is the currency that facilitates future innovation and prosperity. Trustworthy technologies, in turn, represent the foundation on which the scaffolding of a fair and cohesive society is built. Unless we act to improve digital trust with intentional and persistent trust-building initiatives, the digital world will continue to drift towards fragmentation and the promise of one of the most dynamic eras of human progress may be lost.



REUTERS/MAXIM SHEMETOV

Endnotes

1 World Economic Forum, in partnership with Marsh & McLennan Companies, SK Group and Zurich Insurance Group. 2021. The Global Risks Report 2021. Insight Report. Chapter 2 Error 404. Geneva: World Economic Forum. January 2021. https://www.weforum.org/reports/the-global-risks-report-2021

2 World Economic Forum, in partnership with Marsh & McLennan Companies and Zurich Insurance Group. 2020. The Global Risks Report 2020. Insight Report. Chapter 5 Wild Wide Web. Geneva: World Economic Forum. January 2020. https://www.weforum.org/reports/the-global-risks-report-2020

3 Check Point Software Technologies Ltd. 2021. The Biggest Cloud Security Challenges of 2021. https://pages.checkpoint.com/2020-cloud-security-report.html?utm_term=cyber-hub; Kent, J. 2020. "APIs are the next frontier in cybercrime". Security. 3 September 2020. https://www.securitymagazine.com/articles/93239-apis-are-the-next-frontier-in-cybercrime

4 Hoster, B. and Sequeira, T. 2021. Harnessing Technology Convergence: Lessons from Smart Manufacturers. Marsh McLennan. https://www.marshmclennan.com/insights/publications/2021/may/harnessing-technology-convergence.html

5 Allyn, B. 2021. "People are talking about Web3. Is it the Internet of the future or just a buzzword?" National Public Radio. 21 November 2021. https://www.npr.org/2021/11/21/1056988346/web3-internet-jargon-or-future-vision; Clark, P.A. 2021. "The metaverse has already arrived. Here's what that actually means". Time. 15 November 2021. https://time.com/6116826/what-is-the-metaverse/; Robertson, A. and Peters, J. 2021. "What is the metaverse, and do I have to care?" The Verge. 4 October 2021. https://www.theverge.com/22701104/metaverse-explained-fortnite-roblox-facebook-horizon

6 World Economic Forum, in partnership with Marsh & McLennan Companies, SK Group and Zurich Insurance Group. 2021. The Global Risks Report 2021. Insight Report. Chapter 5 Imperfect Markets. Geneva: World Economic Forum. January 2021. https://www.weforum.org/reports/the-global-risks-report-2021

7 Korn, J. 2021. "The Log4j security flaw could impact the entire internet. Here's what you should know". CNN. 15 December 2021. https://edition.cnn.com/2021/12/15/tech/log4j-vulnerability/index.html

8 Reuters Staff. 2021. "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president". Reuters. 15 February 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

9 Burke, S. 2021. "Cyber-crime learnings and predictions for 2021". Counter Terror Business. 15 January 2021. https://counterterrorbusiness.com/features/cyber-crime-learnings-and-predictions-2021

10 Coveware. 2021. "Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021". 21 October 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

11 Help Net Security. 2021. "Malware increased by 358% in 2020". Help Net Security. 17 February 2021. https://www.helpnetsecurity.com/2021/02/17/malware-2020/

12 Chainalysis Team. 2021. "Ransomware 2021: Critical mid-year update". Insights. 14 May 2021. https://blog.chainalysis.com/reports/ransomware-update-may-2021

13 Sharton, B.R. 2021. "Ransomware attacks are spiking. Is your company prepared?" Harvard Business Review. 20 May 2021. https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared; Steib, M. 2021. "What's driving the surge in ransomware attacks?" New York Magazine Intelligencer. 7 September 2021. https://nymag.com/intelligencer/article/ransomware-attacks-2021.html; Pupillo, L. et al. 2021. "Artificial Intelligence and Cyber Security." CEPS Task Force. May 2021. https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf

14 Rosenzweig, P. 2021. "There's a better way to stop ransomware attacks". New York Times (Guest Essay). 31 August 2021. https://www.nytimes.com/2021/08/31/opinion/ransomware-bitcoin-cybersecurity.html

15 Davis, E. and Mee, P. 2021. Growing Cyber Threat Demands a United Response. Marsh McLennan. https://www.marshmclennan.com/insights/publications/2021/october/growing-cyber-threat-demands-a-united-response.html

16 Accenture. 2021. Threats Unmasked: 2021 Cyber Threat Intelligence Report. 2021. https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf; BBC. 2021. "Hacker tries to poison water supply of Florida city". BBC. 8 February 2021. https://www.bbc.com/news/world-us-canada-55989843; European Insurance and Occupational Pensions Authority. 2021. "Cyber risks: what is the impact on the insurance industry?" 15 October 2021. https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en; Poulsen, K., McMillan, R. and Evans, M. 2021. "A hospital hit by hackers, a baby in distress: The case of the first alleged ransomware death". Wall Street Journal. 30 September 2021. https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116; Sganga, N., Herridge, C. and Bidar, M. 2021. "Foreign hacking group targets hospitals, clinics with ransomware attacks, says new report". CBS News. 7 October 2021. https://www.cbsnews.com/news/cyberattacks-ransomware-hacking-hospitals-target-foreign-groups/

17 Accenture. 2021. Op. cit.

18 2021. "Apple sues Israeli firm NSO Group over spyware". Al Jazeera. 23 November 2021. https://www.aljazeera.com/news/2021/11/23/apple-sues-israeli-firm-nso-group-over-spyware

19 Collins, A. and Ebrahimi, T. 2021. "Risk governance and the rise of deepfakes". EPFL International Risk Governance Center. 12 May 2021. https://www.epfl.ch/research/domains/irgc/spotlight-on-risk-series/risk-governance-and-the-rise-of-deepfakes/

20 Cyber Outlook Series virtual workshop on survey results held on 31 March 2021 from Geneva by the Centre for Cybersecurity.

21 Herbert Smith Freehills. 2021. "China's new laws complicate data transfers". 24 August 2021. https://hsfnotes.com/data/2021/08/24/chinas-new-laws-inhibit-data-transfers/

22 Chandrasekhar, C. and Mee, P. 2021. "Why businesses and governments must fight cyber threats together". World Economic Forum Global Agenda. 3 May 2021. https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/

23 Insight. 2021. Cybersecurity at a Crossroads: The Insight 2021 Report. 4 March 2021. https://www.insight.com/content/dam/insight-web/en_US/pdfs/insight/cybersecurity-at-a-crossroads/cybersecurity-at-a-crossroads--the-insight-2021-report.pdf

24 Cf. Tay, S. 2019. "A serious shortage of cybersecurity experts could cost companies hundreds of millions of dollars". CNBC. 5 March 2019. https://www.cnbc.com/2019/03/06/cybersecurity-expert-shortage-may-cost-companies-hundreds-of-millions.html

25 Bloomberg. 2019. "Coalition Secures $40M in Funding to Democratize Access to Cybersecurity". Press Release. 9 May 2019. https://www.bloomberg.com/press-releases/2019-05-09/coalition-secures-40m-in-funding-to-democratize-access-to-cybersecurity

26 Boyd, C. 2021. "Zuckerberg's Metaverse, and the possible privacy and security concerns". Malwarebytes Labs. 2 November 2021. https://blog.malwarebytes.com/privacy-2/2021/11/zuckerbergs-metaverse-and-the-possible-privacy-and-security-concerns/; Department of Homeland Security. 2021. Post-Quantum Cryptography. https://www.dhs.gov/quantum; Kalmann, A. 2018. "Blog: Cyber Security & the Metaverse". IBC365. 22 June 2018. https://www.ibc.org/blog-cyber-security-and-the-metaverse/2904.article

27 Kanterman M. and Naidu N. 2021 "Metaverse may be $800 billion market, next tech platform". Bloomberg Intelligence. 1 December 2021. https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/

28 Steib. 2021. Op. cit.

29 Murgia M. 2021. "Palantir to reshore all UK data processing from US before regulatory 'tsunami' hits". 17 December 2021. https://www.ft.com/content/76fa6a3f-a818-4e88-be14-b578ae378d7c

30 Pocock, J. and O'Brien, S. 2021. Cyber Risk: The Emerging Cyber Threat to Industrial Control Systems. Lloyd's, CyberCube, and Guy Carpenter. 2021. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2021/august/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_Final%2016.02.2021.pdf

31 Verizon. 2020. 2020-2021. Cyber-Espionage Report. https://www.verizon.com/business/resources/reports/2020-2021-cyber-espionage-report.pdfx

32 Buckley, J. and Conner, S. 2021. "Cyber Threats: Living with Disruption". Control Risks and AirMic. 12 October 2021. https://www.controlrisks.com/our-thinking/insights/reports/cyber-threats-living-with-disruption

33 See, e.g., CBS News. 2019. "Doctored Nancy Pelosi video highlights threat of "deepfake" tech". 26 May 2019. https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/

34 Brewster, T. 2021. "Fraudsters cloned company director's voice in $35 million bank heist, police find". Forbes. 14 October 2021. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=af66cf275591

35 Fisher, M. 2021. "Disinformation for hire, a shadow industry, is quietly booming". The New York Times. 25 July 2021. https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html; Joyce, S., Kashifuddin, M., Nocera, J. and Upton, P. 2021. "The disinformation age has arrived. Are you ready?" PwC. 9 February 2021. https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html

36 UK Finance. 2021. Fraud — The Facts 2021. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

37 Moon Sehat, C. 2021. "Advancing digital safety: A framework to align global action". World Economic Forum. June 2021. https://www3.weforum.org/docs/WEF_Advancing_Digital_Safety_A_Framework_to_Align_Global_Action_2021.pdf; Lalani, F. 2021. "Risks to kids online are growing. Here's what we can do". World Economic Forum. 13 October 2021. https://www.weforum.org/agenda/2021/10/overcoming-the-growing-risks-to-kids-online/

38 Braue, D. 2021. "Global cybersecurity spending to exceed $1.75 trillion from 2021-2025". Cybercrime Magazine. 10 September 2021. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/; Meeuwisse, R. 2019. "Is effective cybersecurity expensive?" Infosecurity Magazine. 10 April 2019. https://www.infosecurity-magazine.com/blogs/effective-cybersecurity-expensive

39 Marsh. 2021. Global Insurance Market Index Q3 2021. October 2021. https://www.marsh.com/fr/en/services/insurance-market-and-placement/insights/global_insurance_market_index.html

40 Sabbagh, D. 2021. "Experts say China's low-level cyberwar is becoming severe threat". The Guardian. 23 September 2021. https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat

41 BBC. 2021. "Aukus: UK, US and Australia launch pact to counter China". BBC. 16 September 2021. https://www.bbc.com/news/world-58564837; Kanno-Youngs, Z. and Sanger, D.E. 2021 "U.S. accuses China of hacking Microsoft". The New York Times. 26 August 2021. https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html?; McWhorter, D. 2021. "Exposing one of China's cyber espionage units". Mandiant. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

42 Kemp, S. 2021. "Digital 2021 April Global Statshot Report". Datareportal. 26 April 2021. https://datareportal.com/reports/digital-2021-april-global-statshot

43 Rodriguez, K. and Opsahl, K. 2020. "Augmented reality must have augmented privacy". Electronic Frontier Foundation. 16 October 2020. https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy

44 Sultan, A. 2021. "Improving Cybersecurity Awareness in Underserved Populations". UC Berkeley Center for Long-Term Cybersecurity White Paper Series. 2021. https://cltc.berkeley.edu/underserved_populations/

45 Kite-Powell, J. 2021. "The rise of voice cloning and deepfakes in the disinformation wars". Forbes. 21 September 2021. https://www.forbes.com/sites/jenniferhicks/2021/09/21/the-rise-of-voice-cloning-and-deep-fakes-in-the-disinformation-wars/?sh=405859e138e1; Nicolls, D. 2019. "Will deepfake technology defeat biometric authentication?" Jumio.com. 10 October 2019. https://www.jumio.com/deepfake-technology-biometric-authentication/; Pipikaite, A. 2021. "How to improve security of biometric data". World Economic Forum Global Agenda. 2 September 2021. https://www.weforum.org/agenda/2021/09/untangling-the-benefits-and-risks-of-biometrics/

46 ISACA. 2021. "State of Cybersecurity 2021: Threat Landscape, Security Operations and Cybersecurity Maturity (Part 2)". ISACA. 2021. https://www.isaca.org/go/state-of-cybersecurity-2021; Kite-Powell, J. 2020. "Here's how 2020 created a tipping point in trust and digital privacy". Forbes. 27 October 2020. https://www.forbes.com/sites/jenniferhicks/2020/10/27/heres-how-2020-created-a-tipping-point-in-trust-and-digital-privacy/?sh=7fe5bc4a4fc5; Lucas, O. 2021. "Corporate data responsibility: Bridging the consumer trust gap". PwC. August 2021. https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html?utm_source=vanity&utm_medium=referral&mid=m-00005652&utm_campaign=c-00107353&cid=c-00107353; Muggah, R. 2021. "Digital privacy comes at a price. Here's how to protect it". World Economic Forum Global Agenda. 8 September 2021. https://www.weforum.org/agenda/2021/09/how-to-protect-

digital-privacy/; NortonLifeLock, Inc. 2021. "Norton Cyber Safety Insights Report: Global Results". Norton and The Harris Poll. May 2021. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

47 Statista. Most popular global mobile messenger apps as of October 2021, based on number of monthly active users, accessed 14 December 2021. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

48 Privacy International. 2019. "Most cookie banners are deceptive and annoying. This is not privacy". Privacy International. 21 May 2019. https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent

49 Kwet, M. 2021. "Digital colonialism: The evolution of US empire". TNI's Future Lab series on Technology, Power and Emancipation organized in collaboration with ROAR magazine. 4 March 2021. https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire; Ryan-Mosley, T. 2021. "Why you should be more concerned about Internet shutdowns". MIT Technology Review. 9 September 2021. https://www.technologyreview.com/2021/09/09/1035237/internet-shutdowns-censorship-exponential-jigsaw-google/

50 Buckley, J. and Conner, S. 2021. "Cyber threats: Living with disruption". Control Risks and AirMic. 12 October 2021. https://www.controlrisks.com/our-thinking/insights/reports/cyber-threats-living-with-disruption; 2021. "Insurance giant AXA victim of ransomware attack". Security. 19 May 2021. https://www.securitymagazine.com/articles/95245-insurance-giant-axa-victim-of-ransomware-attack

51 Rappeport, A., Kramer, A.E. and Sanger, D.E. 2021. "The Biden administration is combating ransomware with a crackdown on cryptocurrency payments". The New York Times. 21 September 2021. https://www.nytimes.com/2021/09/21/us/politics/treasury-department-combating-ransomware-cryptocurrency.html; U.S. Securities and Exchange Commission. 2021. "SEC Announces Three Actions Charging Deficient Cybersecurity Procedures". Press Release. 30 August 2021. https://www.sec.gov/news/press-release/2021-169

52 Mee, P. and Brandenburg, R. 2020. "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk". World Economic Forum Global Agenda. 17 December 2020. https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

53 Check Point Software Technologies Ltd. 2021. The Biggest Cloud Security Challenges of 2021. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-native-security/the-biggest-cloud-security-challenges-in-2021/